Summary: Your wallet depends on where you are in your web3 journey, and how much crypto you have to store.

So this article is NOT going to be a:

Top 5 Crypto Wallets to use in web3! (Number 4 will surprise you)

No.

None of that.

This is “Hey, let’s take a practical approach to what wallet serious projects should use.” This will not be an exhaustive summary, as teaching OpSec and threat vectors would be another 60-ish hour-long course. Additionally, we have not personally done security reviews of any of the wallets we will mention, and we ask security-focused users to refer to the security information provided by each option.

However, we looked at the wallet's security reviews and information.

This is the no-BS, no “click here to buy this wallet,” just the facts guide to chose the best web3 wallet, and the safest way to store crypto, for you!

Thank you to

[Trail of Bits

](https://blog.trailofbits.com/2018/11/27/10-rules-for-the-secure-use-of-cryptocurrency-hardware-wallets/)’ and

[officer_cia’s

](https://twitter.com/officer_cia) resources for helping write this guide.

Who is this guide for?

This guide is aimed at beginner/intermediate smart contract developers and protocols, and anyone saying :

“Hey, I’m pretty serious about this Web3 thing, so now I’m getting nervous about where to store my money.”

For example, if you’ve gone through the Cyfrin Updraft Blockchain Basics course -> Advanced Foundry, this guide is for you.

TL;DR: Wallet suggestions based on money amount and experience

- Total Noob:

Custodial wallet / Exchange

- Beginner/Smol money

: Browser

- Intermediate/Medium-Small Money

: Hardware wallet

- Intermediate/Big Money

: Multi-sig wallet/Social Recovery AND Hardware wallet

- Advanced/Big Money

: Multi-sig wallet/Social Recovery or roll your own solution

Quick links:

- Compare wallets site
- Compare desktop & browser wallets

Introduction

Your crypto wallet setup will never be perfect.

Everyone has a different idea of what a great wallet setup is.

Your job is to keep learning, keep growing, and understand the tradeoffs using one approach over another. In technology, most of the time there isn't an "objectively best" way to do something. For wallets, it's the same thing.

And now, our guide.

Web3 wallet setup recommendations

Total noobs: Custodial wallet / Centralized Exchange

Noobs

: Custodial Wallet

A CENTRALIZED PLATFROM, HOW COULD YOU??

I know us recommending a centralized platform amongst the best web3 wallets solutions is true blasphemy. But hear me out. Your friends will ask you what wallet to use, and your recommendation likely should not be the same as what you use.

Think of the dumbest person in your circle of friends/family you know.

Think of the person you've had to explain 100 times what a "smart contract" is and ask yourself—"Would I trust this person to manage their own private keys?"

If the answer is "no," they should use a centralized exchange until they level up.

Note

: At Cyfrin we don't think anyone is "dumb", just "uneducated", but we used the word "dumb" for dramatic effect.

Pros

- Easy to use
- They can protect you if you're not great at using crypto yet

Cons

- The exchange can rug pull you (Not your keys, not your crypto)
- The exchange can go under
- The exchange can freeze your account
- The exchange owns your money
- Doesn't work with web3 apps

Potential Suggestions

- Coinbase
- Kraken

Best Web3 wallets for beginners, small amounts and short term storage

Beginners:

Browser, Desktop, or Hardware

First, a few definitions:

Beginner

: Someone who has finished theSolidity Fundamentals course on Cyfrin Updraft, or has some web3 knowledge is still getting their footing, and wouldn't describe themselves as "comfortable" playing around on Etherscan.

- Small Money:

An amount of money where the world wouldn't end for you if you lost all of it. This is different from person to person. For Jeff Bezos, this is ~$1 million. For some kid from the USA in college who has taken out student loans, this might be $50. For a parent with 2 kids, but a good job, this might be $1,000. This is

an amount of money that you don't want to lose, but if you did, you wouldn't be devastated.

- Short-Term Storage:

Money you plan on holding for a short time. Like cash in a traditional wallet.

- Hot Wallet

: A wallet connected to the internet.

- Cold Wallet

: A wallet not connected to the internet.

First, let's focus on hot wallets as they are arguably less secure than other crypto wallets solutions.

Hot Wallets

After an exchange/custodial wallet, the next step is to "level up" to a more sophisticated web3 wallet, like a browser, desktop, or hardware wallet. If you are a protocol/project/organization, your money should not be in the hands of solely one of these.

These wallets are great for getting started in Web3 and holding real funds like ethereum, bitcoins, or other tokens under our own custody. Browser wallets are great for quickly interacting with apps, and most sites work best with browser wallets.

However, we do not recommend you use these for large amounts of funds, or control of applications.

Having a single point of failure in any system is a security risk, and if your hot wallet is hacked, or your computer is breached, you're screwed! You want as few areas where an attacker can break you, and if access to your wallet is only guarded by a password on your laptop, well you better not take that laptop to any events!

Additionally, having a single user guard the war chest is never a good idea, so we want to use a wallet where moving funds is harder for larger amounts of money. But for small amounts of money and everyday use, this is great.

If you MUST have a lot of money in a hot wallet, it's best to spread the money to multiple wallets with different secret phrases so that if one gets compromised, all is not lost.

What to look for in a good web3 wallet

In a good browser/desktop/hardware crypto wallet, you should look for:

- Security reviews/ratings of the tool
- Whether the tool is open-sourced (open sourced == good)

Pros

- Your keys, your crypto
- Ease of use with web3 apps
- Great for keeping "small" amounts of money, like a real wallet.

Cons

- You are the sole security checkpoint
- If you make a mistake, you can get rekt quick
- Hot wallets mean you're connected to the internet, so if someone hacks your computer, you're rekt!
- Supply chain attacks: You download a bad software/wallet
- Some wallets track your data and you'll need to customize your wallets for more privacy

Potential Suggestions (Hot wallet)

- Metamask
- Rabby
- Frame
- Rainbow
- MyEtherWallet

Suggestions to level up your hot wallet

These are tools that will make using your wallet safer.

- Web3 Antivirus
- fire.xyz

Hardware wallets: best crypto wallet for intermediates, medium monies, medium storage

Intermediates

: Browser, Desktop, or Hardware

First, a quick definition, by Medium Monies

we mean an amount of money that would suck to lose, full stop. But not all your money. This means that big money (

in the next section) is a large percentage of your money.

Ideally, if you're paranoid about your cash (which, you should be) then storing your money in a hardware wallet is your next option

After a browser/desktop web3 wallet, we can level up to a hardware wallet. Ideally, this device is "air-gapped", meaning it has no connection to the internet.

This is a level up from a browser wallet, as it becomes harder for even you to access the crypto. However, if someone gets your device, they could hack it and get your key. In the event someone steals your device, consider it compromised. See more on compromised keys at the bottom.

However, they suffer a lot of the same issues as browser wallets. You are the centralized point, if you mess up, you can lose everything.

Same as a hot wallet, if you MUST have a lot of money in a hot wallet, it's best to spread the money to multiple crypto wallets with different secret phrases so that if one gets compromised, all is not lost. Or use the methodology described in the next section.

Pros

- All the pros of browser wallet
- Separation from the internet
- Good for small to medium amounts of money

Cons

- Vulnerable to "wrench attacks", where someone physically attacks you and steals your device
- Same cons as a browser wallet
- Supply chain attacks: Someone could swap the wallet you ordered with a malicious one, or you download bad software, or they could check out your secret phrase beforehand

Potential Suggestions (Cold wallet)

- Trezor

Multi-signature wallets: Best web3 wallets for advanced users, big monies, long-term storage

Advanced Users:

Multi-sig and social recovery

Multi-Sig Wallets

Multi-sig wallets like Safe are our top choice in this list of best web3 wallets to use, both for advanced developers and protocols to store their funds. The way they work is that you deploy a smart contract that needs X of Y signers to send any transaction. Optionally, Aragon has a multi-sig feature for DAOs specifically.

For example, in a 3 of 5 multi-sig:

- Metmask Wallet A approves to send 5 ETH
- Trezor Wallet B approves to send 5 ETH
- Frame Wallet C approves to send 5 ETH → 3/5 achieved, ETH is sent.

This is a great option for even sole developers and non-developers who want to have safer, longer-term holdings passing various safety checks. You can use a combination of options from above as the signers.

Social Recovery

Social recovery is another great option for more advanced users. This is Vitalik's personal favorite option.

How it works:

1. There is a single "signing key" that can be used to approve transactions
2. There is a set of at least 3 (or a much higher number) of "guardians", of which a majority can cooperate to change the signing key of the account.

From Vitalik's blog:

Under all normal circumstances, the user can simply use their social recovery wallet like a regular wallet, signing messages with their signing key so that each transaction signed can fly off with a single confirmation click much like it would in a "traditional" wallet like Metamask.

If a user loses

their signing key, that is when the social recovery functionality would kick in.

Users could also use a Shamir backup, similar to social recovery. You give out "shares" of your key to trusted users, where you can recover your key when the shares are combined.

A recovery share is usually a sequence of 20 or 33 English words carrying a part of the cryptographic secret. Trezor T is a hardware wallet that comes out of the box with this feature.

Pros

- Many signers, meaning multiple steps to take actions
- If a key is compromised, you don't have to move funds, you swap out the compromised key

Cons

- Weak support from web3 apps
- The address is different on different chains

Potential Suggestions (Multi-sig)

- Safe

Potential Suggestions (Social Recovery)

- Safe
- Argent

Self-made tools Best crypto wallets for super advanced users - safest way to store your crypto

Super Advanced Users:

Self-tools

Each of the options above have issues.

One way or another, there is no perfect solution when it comes to choosing the safest way to store your crypto. So, some people decide to go the extra mile due to their lack of trust (justifiably) in each of the cons from above.

So there are some options others take:

- Brain wallet:

A user only uses their private key that they have committed to memory

- Paper wallet:

A user only uses their private key that they have written on a piece of paper in a safe location

- Self-encryption tools:

A user has created their own encryption tools and/or password managers that they use anytime they send transactions.

I met someone once who had a system that looked like this:

- Had hundreds of wallets with small amounts, each with their backups stored in different locations, and about 10 “main” ones with “most” of their money
- Never used hardware or browser wallets, didn’t trust them, and generated the secret phrases from tools they themselves built
- Encrypted each key, and stored the encrypted keys in a secret database on a select few hard drives stored in secret locations with trusted individuals (like a sudo social recovery, the people they sent the devices to had no idea how to decrypt them)
- Every 6 months, they would rotate all the money around to different and new wallets

So, you can also do something like this when you get wealthy, or have a lot of money to protect.

Pros

- You don’t have to trust anything, except yourself

Cons

- This takes a lot of time and a very advanced user

Safe ways to store your crypto: Key management and good private key habits

1. Should I tell people how much money I have?

No.

Step 1 of any attacker is to pick a target. The lower profile you have, the better. The less information an attacker can get on you, the better.

1. Should I get a hardware wallet from a hackathon?

No.

Here are some tips for dealing with hardware wallets securely:

a) Always buy directly from the vendor/company—or official resellers. But make sure the official reseller is actually official.

b) Do not use a hardware wallet you got from a hackathon

1. Can I use the same private key for years?

You can, but it’s best to rotate your keys/wallets. Swap them out for different ones. This is why a multi-sig wallet like Safe is great, you can keep the same address/wallet but change the signers.

Ideally, every 6 months or so (depending on your security hygiene) you should do a security review of your keys.

- Where are all my keys?
- Where is all my money?
- If my house burns down (including my phone/computer), will I be able to recover my crypto?

Exercise: Take out your calendar and set a recurring event where you review your keys every 6 months.

1. Where do I back up my secret phrase / private key?

You can/should back it up in a secret spot only you know. Something like the following:

- Place it on metal plates and hidden
- Commit it to memory
- Written on a piece of paper in a secret spot
- Encrypted in a password manager (do NOT let the password manager know the private key/secret phrase)
- Stick it in a vault

There are many places to securely store your private key/secret phrase, which is good. We want to make knowledge about it difficult. This is where you can/should get a little creative.

1. What should I NOT do with my private key/secret phrase?
2. Take a photo of it
3. Upload it to the cloud
4. Text it
5. Email it
6. Give it to your cousin Jared, who is known for gossiping about
7. Does my OS matter?

Yes. Don't use PC/Windows to store/do anything with any serious amounts of crypto. Windows is the target of the most malware on the planet and its security permissions are arguably less intuitive.

AND MOST IMPORTANTLY

If, for even 1 second, your key is:

- Lost
- Shown on screen
- Potentially accessible by someone else

Consider it compromised, and start moving your money to a new wallet.

To learn smart contract security and development, visit

[Cyfrin Updraft

](https://updraft.cyfrin.io/).

To request security support/security review for your smart contract project visit

[Cyfrin.io

](https://cyfrin.io/)or

[CodeHawks.com

](https://codehawks.com/).